

OpenBSD

Daniel Plakosh, Software Engineering Institute [vita¹]

Copyright © 2005, 2008 Pearson Education, Inc.

2005-09-27; Updated 2008-10-06

L3 / D/P, L²

The OpenBSD UNIX variant was designed with an additional emphasis on security. In particular, OpenBSD adopted phkmalloc and adapted it to support guard pages and randomization.

Development Context

Dynamic memory management

Technology Context

C++, C, OpenBSD

Attacks

Attacker executes arbitrary code on machine with permissions of compromised process or changes the behavior of the program.

Risk

Standard C dynamic memory management functions such as `malloc()`, `calloc()`, and `free()` [ISO/IEC 99] are prone to programmer mistakes that can lead to vulnerabilities resulting from buffer overflow in the heap, writing to already freed memory, and freeing the same memory multiple times (e.g., double-free vulnerabilities).

Description

The OpenBSD UNIX variant was designed with an additional emphasis on security. OpenBSD adopted phkmalloc and adapted it to support guard pages and randomization. Table 1 shows some of the additional security options added for the OpenBSD version of phkmalloc. The default options are AJ.

Table 1. OpenBSD additional phkmalloc options

Flag	Description
F	“Freeguard.” Enables use after free protection. Unused pages on the freelist are read and write protected to cause a segmentation fault upon access.
G	“Guard.” Enables guard pages and chunk randomization. Each page size or larger allocation is followed by a guard page that will cause a segmentation fault upon any access. Smaller than page-size chunks are returned in a random order.

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/268-BSI.html (Plakosh, Daniel)

References

[ISO/IEC 99]

ISO/IEC. *ISO/IEC 9899 Second edition 1999-12-01 Programming Languages — C*. International Organization for Standardization, 1999.

Pearson Education, Inc. Copyright

This material is excerpted from *Secure Coding in C and C++*, by Robert C. Seacord, copyright © 2006 by Pearson Education, Inc., published as a CERT® book in the SEI Series in Software Engineering. All rights reserved. It is reprinted with permission and may not be further reproduced or distributed without the prior written consent of Pearson Education, Inc.